CLAIMS

What is claimed is:

Sub a1

1. A method for use in verifying the integrity of a remote unit in a communication system, said method comprising:

generating a random value;

determining memory range information identifying a range of memory space within the remote unit having data to be hashed by a hashing function;

determining position information indicative of a position within a data stream to be generated within the remote unit at which said random value is to be located; and

delivering said random value, said memory range information, and said position information to the remote unit for use by the remote unit in performing a hashing operation.

2. The method claimed in claim 1, further comprising the step of:

receiving a hash value from said remote unit, said hash value being a result of a hashing operation performed within said remote unit based upon said random value, said memory range information, and said position information delivered to the remote unit.

3. The method claimed in claim 2, further comprising the step of:

comparing said hash value received from said remote unit to a hash value generated outside said remote unit to determine whether modifications have been made within said remote unit.

4. The method claimed in claim 3, wherein:

said hash value generated outside said remote unit is generated within a communication unit that is a replica of said remote unit.

5. The method claimed in claim 3, wherein:

said hash value generated outside said remote unit is a result of a hashing operation performed outside the remote unit based upon said random value, said memory range information, and said position information.

6. The method claimed in claim 1, wherein:

said steps of generating, determining memory range information, determining position information, and delivering are performed in a location that is different from the location of said remote unit.

7. A computer readable medium having program instructions stored thereon for use in implementing the method of claim 1 when executed within a digital processing device.

8. A communication apparatus for use in verifying the integrity of a remote unit in a communication system, comprising:

a random value generator for generating a random value;

a memory range determination unit for determining memory range information identifying a memory range within the remote unit for use in generating a data stream that will be processed by a hashing function within the remote unit;

a location determination unit for determining location information that is indicative of a position within the data stream generated within the remote unit at which said random value is to be located; and

a transmitter for transmitting said random value, said memory range information, and said location information to the remote unit for use in performing a hashing operation therein.

9. The communication apparatus of claim 8, further comprising:

an interrogation message assembly unit for generating an interrogation message including said random value, said memory range information, and said location information.

10. The communication apparatus of claim 9, wherein:

said transmitter transmits said interrogation message to the remote unit via a communication network.

11. The communication apparatus of claim 8, further comprising:

a local memory storing information that is representative of information that should be stored in the remote unit; and

a hash unit for performing a hashing operation on information stored within said local memory to generate a control value, said hashing operation being performed using said random value, said memory range information, and said location information.

12. The communication apparatus of claim 11, further comprising:

a receiver for receiving a hash value from the remote unit, said hash value having been generated within the remote unit by performing a hashing operation within the remote unit based upon said random value, said memory range information, and said location information.

13. The communication apparatus of claim 12, further comprising:

a comparison unit for comparing the hash value received from the remote unit to the control value generated by the hash unit.

14. The communication apparatus of claim 8, further comprising:

a selection unit for selecting a hashing algorithm from a plurality of hashing algorithms for use by the remote unit to perform said hashing operation; and

means for indicating a selected hashing algorithm to the remote unit.

15. A communication unit for use within a communication system comprising:

means for receiving an integrity verification request from a requesting entity, said

integrity verification request including a random value, placement information indicating a desired position for said random value within a data stream, and memory range information identifying a memory range within the communication unit that is to be processed using a hashing function;

means for generating a data stream using data from said memory range and said random value, said random value being located within said data stream at a position indicated by said placement information;

means for performing a hashing operation on said data stream to generate a hash value; and

means for transmitting said hash value to said requesting entity.

16. The communication unit claimed in claim 15, wherein:

said means for generating a data stream includes means for storing said random value in a memory location within said communication unit corresponding to said placement information and means for reading data from said memory range of said communication unit indicated within said integrity verification request to generate said data stream.

17. The communication unit claimed in claim 15, wherein:

said means for generating a data stream includes means for reading data from said memory range of said communication unit to generate a first data stream and

means for inserting said random value into said first data stream at a position indicated by said placement information to generate a second data stream.

18. The communication unit claimed in claim 15, further comprising:

means for receiving a hashing algorithm from said requesting entity for use by said means for performing a hashing operation.